UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,021	11/12/2003	Arnaud Fausse	09669/009002	6206

22511 7590 09/22/2010		

OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER
REZA, MOHAMMAD W

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
09/22/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
buta@oshaliang.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/706,021	FAUSSE, ARNAUD
	Examiner	Art Unit	
	MOHAMMAD W. REZA	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2010*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *7-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

1. This is in response to the arguments filed on 07/06/2010.

2. Claims 7-20 are pending in the application.

3. Claims 7-20 have been rejected.

Response to Amendment

4.   The examiner approves the amendments made to claims 7-11, and 13-14.

5.   The examiner approves cancellation of claims 1-6.

Response to Arguments

5.   Applicant's arguments filed on 07/06/2010 have been fully considered but they
are not persuasive.

Applicant raises mainly two major arguments as follows:

A.   Applicant argues that the Sedlak's "data carrier read/write device" is not a
protected device. Examiner respectfully reminds that the applicant mistakenly
misunderstood and misinterpreted Sedlak's invention. There are several places in
Sedlak's invention wherein it clearly mentions the "data carrier read/write device" which
is connected with the data generation device (similar to the "message storage device" of
the claim) and display device is act as a "protected device". For example, "the data
carrier read/write device is for receiving a portable data carrier storing a user-specific
key and an algorithm used **to generate** *an electronic signature* (col. 2, lines 26-29,
emphasis added)", "the data carrier read/write device **is configured to** *encrypt the data*

that has been transmitted to the data carrier read/write device (col. 2, lines 38-39,

emphasis added)", clearly shows that the alleged "data carrier read/write device" is

acting as a protected device. Therefore, examiner stuns by the applicant allegation that

"the examiner has <u>mischaracterized</u> Sedlak's smart card reader as a protected device".

On the contrary, applicant intentionally (wrongly) interprets Sedlak's "data carrier

read/write device" is just a "smart card reader". In deed, "data carrier read/write device"

is more than just a "smart card reader" as applicant thought because it is capable of

"generating the electronic signature" and "configured to encrypt the data that it

receives". Therefore, Sedlak's "data carrier read/write device" is definitely acting as a

"protected device" to any ordinary skill in the art who is familiar with the general

meaning of "protected device".

B. Applicant argues that the Sedlak fails to disclose two physically separate links.

Specifically, applicant argues that the there is <u>no link</u> between "data carrier read/write

device" (applicant alleged "smart card" device) and display device (Remarks, dated

07/06/2010, paragraph, B). Examiner again respectfully disagrees with applicant

misunderstanding of the Sedlak's invention. Therefore, showing the comparison figures

of the applicant own specification's figure and Sedlak's invention figure should eliminate

all doubt and misunderstandings. This comparison will give a clear view how the

applicant's application and Sedlak's invention are similar. This will show how the

hardware components (message storage device, protected device, and display device)

are located in exactly the same way in both inventions. The first figure is applicant's own

specification figure and second figure is Sedlak's figure. It is clearly show that the there

is a link between the read/write device (protected device) and display device in Sedlak's

invention. Further, it clearly shows that the first link (link between data generating device

and read/write device) and second link (link between display device and read/write

device) are physically separated.
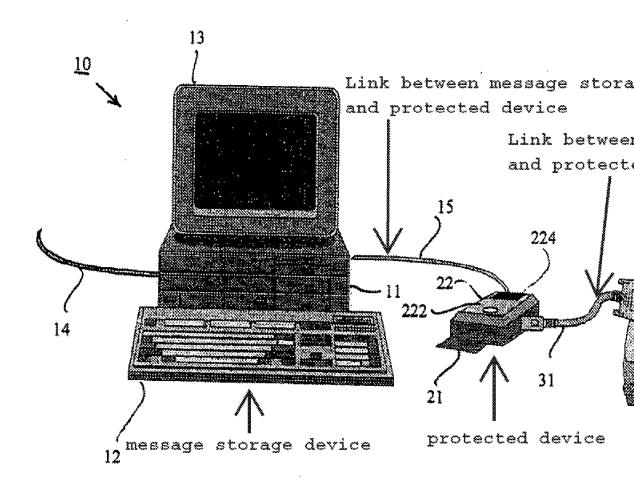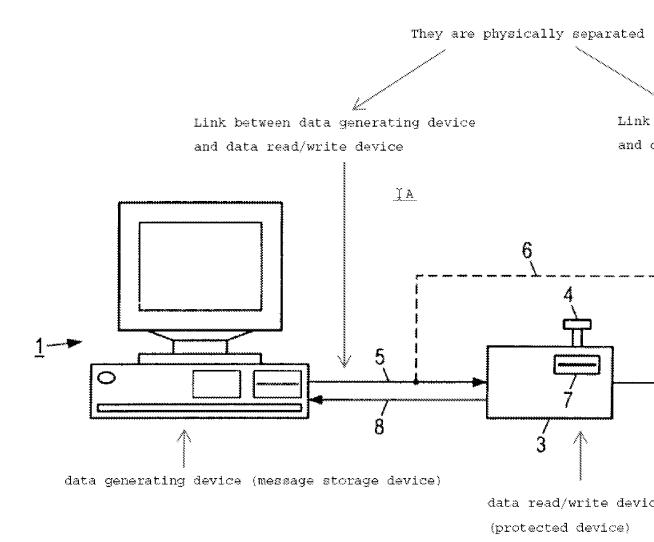
Applicant's own figure:

13

10

Link between message stora
and protected device

Link betweer
and protecte

15

224

22

11

222

14

21

31

message storage device

protected device

12

Figure 1

Sedlak's figure:

They are physically separated

Link between data generating device
and data read/write device

Link
and d

IA

6

4

1→

5

7

8

3

data generating device (message storage device)

data read/write devic

(protected device)

The other arguments regarding the dependent claims are already addressed in the

previous action. Therefore, after carefully reviewing all the arguments examiner

respectfully traverses the applicant's arguments and the rejection will be sustained.

Claim Rejections - 35 USC § 103

17.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

18.   Claims 7-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Holger Sedlak hereafter Sedlak (US Patent 6,510,514) in view of Devaux et al hereafter

Devaux (US Patent 6,769,620).

19.   As per claim 7, Sedlak discloses an authentication device of a message **(Fig.,**

col. 2, lines 23-26, wherein it states that a device for reliably creating the

electronic signature of data includes a data generating device, a data carrier

read/write device, and data display device and this data signature is used to

verify the integrity of the data) comprising

a message storage device **(fig., element 1, col. 2, lines 24-25, "a data generating**

device" which is actually a personal computer (PC) considers as "a message

storage device" as well),

a protected device connected to said message storage device, the protected device

configured to ensure protection of the message **(Fig., element 3, col. 2, lines 26-33,**

"the data carrier read/write device" considers as a "protected device" which is

connected to the PC (message storage device). Further, col. 3, lines 25-26

discuss that this device is certified by an approved authority and sealed which

means protected and it assures protection of the data that travels from data

generating device to the display device);

a display device connected to said protected device (**fig., element 2, col. 2, lines 31-33, wherein it states that the display device is connected to the data generating device through the data carrier read/write device (protected device)**), wherein the protected device is constituted by a card (**col. 4, lines 6-12, wherein it discloses that read/write device (protected device) has an insertion slot to constitute a smart card**) provided with inputs/outputs I1/01 of commands/data for the link with said message storage device (**Fig., elements 5, and 8, col. 2, lines 43-45, wherein it shows that the data generating device (message storage device i.e. PC) is connected with the data carrier device (protected device) through the read/write link and the connection is input/output basis according to the figure**) and input/output I2/02 of display for a second link with said display device (**fig., element 5, col. 2, lines 43-48, wherein it shows that data carrier read/write device (protected device) is connected with the display device through the link. Moreover, col. 4, lines 14-15 states that this connection link could be bidirectional that means it could be input and output both**), wherein the first and second links are physically separate (**it is to be mentioned that Fig. of Sedlak's invention has significant similarity with the fig.1 of the present application by which it shows that the two input/output connections with the data carrier read/write device (Figure, element 3, protected device) with the two specific devices (Figure, element 1 data generating device i.e. message storage device and element 2 display device) are physically separated. Moreover, col. 2, lines 43-45 mention that the protected**

device is located in between the storage device and display device and thus their

connection are physically separated),

wherein the protected device is configured to hash the message received from the

message storage device and to send the message to the display device **(col. 2, lines**

26-33, wherein it discusses that the data carrier device (protected device)

generates the signature of the received data from the data generating device

(storage device) and transmits that data to the display device. The signature of

the encrypted data is the hash of the data which is discussed in col. 1, lines 16-

22. Further, col. 4, lines 7-12 also mentions that the data that receives from the

data storage device is encrypted and signed by the protected device).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes

with smart card and it is well known that the smart card has the embedded

microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is

constituted by a microprocessor. However, in the same field of endeavor, Devaux

discloses that the smart card includes the microprocessor (**fig.1, elements 20, and 220,**

col. 1, lines 4-7, wherein it discusses that the IC card (smart card) has a

microcontroller (microprocessor)).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Sedlak's smart card with a microprocessor as suggest by

Devaux. The motivation is that a number of advantages can be obtained; for one, using

a microprocessor in the card can run its own program to execute the specific

applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may

prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

20.   As per claim 8, Sedlak discloses the authentication device, characterized in that the only logic link between the commands/data circulating between said protected device and said message storage device on one hand and data circulating between said protected device and said display device on the other hand (**Figure, elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data generating device (message storage device) and data carrier read/write device (protected device) in one side and link between display device and data carrier read/write device (protected device) in another side of the protected device and they are based on the data carrying logic)**, is the software of said protected device (**col. 4, lines 8-12, wherein it states that algorithm of the smart card to processes the data that transmitted from the data generating device**).

21.   As per claim 9, Sedlak discloses the authentication device characterized in that said display device is a printer, a screen, or a filing device (**col. 3, lines 7-8, wherein mentions that the displaying device could be a printer, a screen**).

22.   As per claim 10, Sedlak discloses a card (**col. 4, lines 6-12, wherein it states a smart card**) able to be connected to a message storage device and to a display device (**col. 2, lines 29-33, wherein it states that the card reading device is connected with the data generating device (message storage device) and to a display device**), characterized in that it is provided with inputs/outputs I1/01 of commands/data

for the link with said message storage device (**Fig., elements 5, and 8, col. 2, lines 43-**
45, wherein it shows that the data generating device (message storage device i.e.
PC) is connected with read/write link of the data carrier device (protected device)
and the connection is input/output basis according to the figure) and I2/02 of
display for the link with said display device (**fig., element 5, col. 2, lines 46-48,**
wherein it states that data carrier read/write device (protected device) is
connected with the display device through the link. Moreover, col. 4, lines 14-15
states that this connection link could be bidirectional that means it could be input
and output both), physically separate (**it is to be mentioned that Fig. of Sedlak's**
invention has significant similarity with the fig:1 of the present application by
which it shows that the two input/output connections with the data carrier device
(Figure, element 3, protected device) with the two specific devices (Figure,
element 1 data generating device i.e. message storage device and element 2
display device) are physically separated. Moreover, col. 2, lines 43-45 mention
that the protected device is located in between the storage device and display
device and thus their connection are physically separated), and
characterized in that the only logic link between the commands/data circulating between
said card and said message storage device on one hand and data circulating between
said card and said display device on the other hand (**Figure, elements 8, 5, col. 2,**
lines 27-33, wherein it mentions that the link between data generating device
(message storage device) and data carrier read/write device (protected device) in
one side of the protected device and link between display device and data carrier

read/write device (protected device) in another side and they are based on the

data carrying logic), is the software of said card (col. 4, lines 8-12, wherein it states

that algorithm of the smart card to processes the data that transmitted from the

data generating device),

wherein the card is configured to hash the message received from the message storage

device and to send the message to the display device (**col. 2, lines 26-33, wherein it**

discusses that the data carrier device (protected device) generates the signature

of the received data from the data generating device (storage device) and

transmits that data to the display device. The signature of the encrypted data is

the hash of the data which is discussed in col. 1, lines 16-22. Further, col. 4, lines

7-12 also mentions that the data that receives from the data storage device is

encrypted and signed by the protected device).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes

with smart card and it is well known that the smart card has the embedded

microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a

microprocessor card. However, in the same field of endeavor, Devaux discloses that the

smart card (IC card) is a microprocessor card (**fig.1, elements 20, and 220, col. 1,**

lines 4-7, wherein it discusses that the IC card has a microcontroller

(microprocessor)).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Sedlak's smart card with a microprocessor as suggest by

Devaux. The motivation is that a number of advantages can be obtained; for one, using

a microprocessor in the card can run its own program to execute the specific applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

23.   As per claim 11, Sedlak discloses the card, characterized in that the only logic link between the commands/data circulating between said card and said message storage device on one hand and data circulating between said card and said display device on the other hand (**Figure, elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data generating device (message storage device) and data carrier read/write device (protected device) in one side and link between display device and data carrier read/write device (protected device) in another side and they are based on the data carrying logic**), is the software of said card (**col. 4, lines 8-12, wherein it states that algorithm of the smart card to processes the data that transmitted from the data generating device**).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes with smart card and it is well known that the smart card has the embedded microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a microprocessor card. However, in the same field of endeavor, Devaux discloses that the smart card (IC card) is a microprocessor card (**fig.1, elements 20, and 220, col. 1, lines 4-7, wherein it discusses that the IC card has a microcontroller (microprocessor)**).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Sedlak's smart card with a microprocessor as suggest by

Devaux. The motivation is that a number of advantages can be obtained; for one, using

a microprocessor in the card can run its own program to execute the specific

applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may

prompt variations of it for use in either the same field or a different one based on design

incentives or other market forces/market place incentives if the variations are

predictable to one of ordinary skill in the art.

24. As per claim 12, Sedlak discloses the card, characterized in that it comprises a

physically separate inlet to enter a confidential code (**col. 4, lines 6-12, wherein it**

describes that the protected device has separate slot to place the card and

though the encrypted data transmitted from the data creation device).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes

with smart card and it is well known that the smart card has the embedded

microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a

microprocessor card. However, in the same field of endeavor, Devaux discloses that the

smart card (IC card) is a microprocessor card (**fig.1, elements 20, and 220, col. 1,**

lines 4-7, wherein it discusses that the IC card has a microcontroller

(microprocessor)).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Sedlak's smart card with a microprocessor as suggest by

Devaux. The motivation is that a number of advantages can be obtained; for one, using

a microprocessor in the card can run its own program to execute the specific

applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may

prompt variations of it for use in either the same field or a different one based on design

incentives or other market forces/market place incentives if the variations are

predictable to one of ordinary skill in the art.

25.   As per claim 13, Sedlak discloses a box able to receive a protected device and

able to be connected to a message storage device and to a display device (**col. 2, lines

29-33, wherein it states that the card reading device is connected with the data

generating device (message storage device) and to a display device**),

characterized in that it comprises a data/command link with said message storage

device (**Fig. 1, elements 5, and 8, col. 2, lines 43-45, wherein it shows that the data

generating device (message storage device i.e. PC) is connected with read/write

link of the data carrier device (protected device**) and the connection is input/output

based according to the figure) and the link with said display device (**fig. 1, element 5,

col. 2, lines 46-48, wherein it states that data carrier read/write device (protected

device) is connected with the display device through the link. Moreover, col. 4,

lines 14-15 states that this connection link could be bidirectional that means it

could be input and output both**), the inlets/outlets of said data/command link and said

display link being electrically independent (**it is to be mentioned that Fig.1 of this

reference has significant similarity with the fig:1 of the present application by

which it shows that the two links connected with the data carrier device (element

3, protected device) with the two specific devices (element 1 data generating**

device i.e. message storage device and element 2 display device) are being

electrically independent if there is no smart cart in the slot), and

characterized in that the only logic link between the data circulating in the

data/commands and display device (**Figure, elements 8, 5, col. 2, lines 27-33,**

wherein it mentions that the link between data generating device (message

storage device) and data carrier read/write device (protected device) in one side

and link between display device and data carrier read/write device (protected

device) in another side and they are based on the data carrying logic) is the

software of said protected device (**col. 4, lines 8-12, wherein it states that algorithm**

of the smart card to processes the data that transmitted from the data generating

device),

wherein the protected device is configured to hash the message received from the

message storage device and to send the message to the display device (**col. 2, lines**

26-33, wherein it discusses that the data carrier device (protected device)

generates the signature of the received data from the data generating device

(storage device) and transmits that data to the display device. The signature of

the encrypted data is the hash of the data which is discussed in col. 1, lines 16-

22. Further, col. 4, lines 7-12 also mentions that the data that receives from the

data storage device is encrypted and signed by the protected device).

Although, Sedlak discloses a data generating device and a display device are

connected with the protected device. But he does not expressly mention data/command

circuit and a display circuit in the protected device. However, in the same field of

endeavor, Devaux discloses that the data/command circuit and a display circuit in the

protected device (**fig.1, col. 2, lines 8-15, wherein it shows that the card reader has**

circuit for data storage and display devices).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Sedlak's protected device with the circuit for data and

display devices as suggest by Devaux. The motivation is that a number of advantages

can be obtained; for one, using the circuit for data and display device in the card reader

for better control of operation in the reader device (**Devaux col. 2, lines 8-15**). Known

work in one field of endeavor may prompt variations of it for use in either the same field

or a different one based on design incentives or other market forces/market place

incentives if the variations are predictable to one of ordinary skill in the art.

26.   As per claim 14, Sedlak discloses the box, characterized in that the only logic link

between the data circulating in the data/commands and display device (**Figure,**

elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data

generating device (message storage device) and data carrier read/write device

(protected device) in one side and link between display device and data carrier

read/write device (protected device) in another side and they are based on the

data carrying logic) is the software of said protected device (**col. 4, lines 8-12,**

wherein it states that algorithm of the smart card to processes the data that

transmitted from the data generating device).

Although, Sedlak discloses a data generating device and a display device are

connected with the protected device. But he does not expressly mention data/command

circuit and a display circuit in the protected device. However, in the same field of
endeavor, Devaux discloses that the data/command circuit and a display circuit in the
protected device (**fig.1, col. 2, lines 8-15, wherein it shows that the card reader has
circuit for data storage and display devices**).

It would have been obvious to one having ordinary skill in the art at the time the
invention was made to modify Sedlak's protected device with the circuit for data and
display devices as suggest by Devaux. The motivation is that a number of advantages
can be obtained; for one, using the circuit for data and display device in the card reader
for better control of operation in the reader device (**Devaux col. 2, lines 8-15**). Known
work in one field of endeavor may prompt variations of it for use in either the same field
or a different one based on design incentives or other market forces/market place
incentives if the variations are predictable to one of ordinary skill in the art.

27.   As per claim 15, Sedlak discloses the box characterized in that it is allowing to
enter data, such as a confidential code (**col. 2, lines 23-31, wherein it discusses that
the read/write carrier device (protected device) is configured to receive secure
data**). But, Sedlak does not disclose the box characterized in that it comprises a
keyboard. However in the same field of endeavor, Devaux discloses the box
characterized in that it comprises a keyboard (**figure 1, element 12, col. 2, lines 57-60,
wherein it shows that the card reader has a keyboard interface to enter the data**).

It would have been obvious to one having ordinary skill in the art at the time the
invention was made to modify Sedlak's protected device with a keyboard as suggest by
Devaux. The motivation is that a number of advantages can be obtained; for one, using

the keyboard in the card reader for better control of operation in the reader device and data input flexibility (**Devaux col. 2, lines 57-60**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

28.   As per claim 16, Sedlak discloses an authentication device of a message (**Fig., col. 2, lines 23-26, wherein it states that a device for reliably creating the electronic signature of data includes a data generating device, a data carrier read/write device, and data display device and this data signature is used to verify the integrity of the data**), comprising

a storage device (**fig. 1, element 1, col. 2, lines 24-25, "a data generating device" which is actually a personal computer (PC) considers as a message storage device as well**),

a protected device connected to said storage device, the protected device configured to ensure protection of the message (**Fig:1, element 3, col. 2, lines 26-33, "the data carrier read/write device" considers as a "protected device" which is connected to PC (message storage device. Further, col. 3, lines 25-26 discuss that this device is certified by an approved authority and sealed which means protected) and it assures protection of the data that travels from data generating device to the display device**);

a display device connected to said protected device to form a secure environment (**fig.1, element 2, col. 2, lines 31-33, wherein it states that the display device is**

connected to the data generating device through the data carrier device

(protected device)),

wherein the protected device comprises a card (**col. 4, lines 6-12, wherein it**

discloses that read/write device (protected device) has an insertion slot to

constitute a smart card), the card being configured to form a bridge between the

storage device and the display device (**(col. 4, lines 6-12, wherein it states that the**

smart card of the protected device connects the data generating device (message

storage device). Further, col. 2, lines 43-46 discusses that the protected device

connected in between storage device and display device and bridges between

them),

wherein the protected device is configured to hash the message received from the

storage device and to send the message to the display device (**col. 2, lines 26-33,**

wherein it discusses that the data carrier device (protected device) generates the

signature of the received data from the data generating device (storage device)

and transmits that data to the display device. The signature of the encrypted data

is the hash of the data which is discussed in col. 1, lines 16-22. Further, col. 4,

lines 7-12 also mentions that the data that receives from the data storage device

is encrypted and signed by the protected device), and

wherein the storage device is an uncertain zone (**col. 3, lines 60-61, wherein it**

mentions that the PC is used as a data creation device (storage device) and this

data is not certain) and the display device is a certain zone (**col. 3, lines 3-13, this**

elaborates that the display device is checking the correctness of the data which

considers as a certain zone. But, a PC can not do that which is uncertain region).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes

with smart card and it is well known that the smart card has the embedded

microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is

constituted by a microprocessor. However, in the same field of endeavor, Devaux

discloses that the smart card includes the microprocessor (**fig.1, elements 20, and 220,**

col. 1, lines 4-7, wherein it discusses that the IC card (smart card) has a

microcontroller (microprocessor)).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Sedlak's smart card with a microprocessor as suggest by

Devaux. The motivation is that a number of advantages can be obtained; for one, using

a microprocessor in the card can run its own program to execute the specific

applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may

prompt variations of it for use in either the same field or a different one based on design

incentives or other market forces/market place incentives if the variations are

predictable to one of ordinary skill in the art.

29.   As per claim 17, Sedlak discloses the authentication device, wherein the display

device is configured to display the message received from the protected device, and

wherein the message displayed by the display device corresponds to the message

hashed by the protected device (**col. 4, lines 22-28, wherein it discloses that the**

data shown to the display device is coming from the read/write device (protected

device) and that data is secured by the protected device. Thus, it ensures that the

data shown in the display device and data received from the protected device are

identical).

30.   As per claim 18, Sedlak discloses the card, wherein the display device is

configured to display the message received from the card, and wherein the message

displayed by the display device corresponds to the message hashed by the

microprocessor card (**col. 4, lines 22-28, wherein it discloses that the data shown to**

the display device is coming from the read/write device (protected device) and

that data is secured by the protected device. Thus, it ensures that the data shown

in the display device and data received from the protected device are identical).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes

with smart card and it is well known that the smart card has the embedded

microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a

microprocessor card. However, in the same field of endeavor, Devaux discloses that the

smart card (IC card) is a microprocessor card (**fig.1, elements 20, and 220, col. 1,**

lines 4-7, wherein it discusses that the IC card has a microcontroller

(microprocessor)).

It would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Sedlak's smart card with a microprocessor as suggest by

Devaux. The motivation is that a number of advantages can be obtained; for one, using

a microprocessor in the card can run its own program to execute the specific

applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may

prompt variations of it for use in either the same field or a different one based on design

incentives or other market forces/market place incentives if the variations are

predictable to one of ordinary skill in the art.

31.   As per claim 19, Sedlak discloses the box, wherein the display device is

configured to display the message received from the protected device, and wherein the

message displayed by the display device corresponds to the message hashed by the

protected device (**col. 4, lines 22-28, wherein it discloses that the data shown to the**

display device is coming from the read/write device (protected device) and that

data is secured by the protected device. Thus, it ensures that the data shown in

the display device and data received from the protected device are identical).

32.   As per claim 20, Sedlak discloses the authentication device, wherein the display

device is configured to display the message received from the protected device, and

wherein the message displayed by the display device corresponds to the message

hashed by the protected device (**col. 4, lines 22-28, wherein it discloses that the**

data shown to the display device is coming from the read/write device (protected

device) and that data is secured by the protected device. Thus, it ensures that the

data shown in the display device and data received from the protected device are

identical).

Conclusion

24.   THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final

action is set to expire THREE MONTHS from the mailing date of this action. In the

event a first reply is filed within TWO MONTHS of the mailing date of this final action

and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date

the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will the

statutory period for reply expire later than SIX MONTHS from the mailing date of this

final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Mohammad w. Reza whose telephone number is 571-

272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, **MOAZZAMI NASSER G** can be reached on **(571)272-4195**. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

/Nasser Moazzami/   /Mohammad W Reza/
Supervisory Patent Examiner, Art Unit 2436   Examiner, Art Unit 2436